ADOPTED

BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

19 May 10, 2016

LORI GLASGOW
EXECUTIVE OFFICER

Health Services
LOS ANGELES COUNTY

313 N. Figueroa Street, Suite 912
Los Angeles, CA 90012

Tel: (213) 240-8101
Fax: (213) 481-0503

www.dhs.lacounty.gov

To ensure access to high-quality, patient-centered, cost-effective health care to Los Angeles County residents through direct services at DHS facilities and through collaboration with community and university partners.

www.dhs.lacounty.gov

May 10, 2016

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

APPROVAL OF AMENDMENTS TO THREE AGREEMENTS FOR SERVICES SUPPORTING REVENUE MANAGEMENT PROGRAMS (ALL SUPERVISORIAL DISTRICTS) (3 VOTES)

SUBJECT

Request approval of amendments to extend the terms of three agreements for the continued support of revenue management programs administered by the Departments of Health Services and Public Health.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of Health Services (Director), or his designee, to execute Amendment No. 9 to Agreement No. H-703466 with Sutherland Healthcare Solutions, Inc. (Sutherland), effective upon Board approval, to extend the Agreement term for the period from June 1, 2016 through May 31, 2017, for the continued provision of Financial Management Services (FMS) to the Department of Health Services (DHS) and Department of Public Health (DPH) with no change to the compensation rates.

2. Authorize the Director, or his designee, to execute Amendment No. 8 to Agreement No. H-702058 with USCB, Inc. (USCB), effective upon Board approval, to extend the Agreement term for the period June 1, 2016 through May 31, 2017, for the continued provision of Financial Billing and Recovery Services (FBRS) with no change to the compensation rates.

3. Authorize the Director, or his designee, to execute Amendment No. 6 to Agreement No. H-703452 with Nemadji Research Corporation (Nemadji),

effective upon Board approval, to extend the Agreement term for the period from September 1, 2016 through August 31, 2017 for the continued provision of Final Third Party Safety Net and Recovery Services (FTPSNRS) with no change to the compensation rates.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

DHS uses a variety of financial services contractors, including the three referenced above, to support DHS revenue management programs. DPH uses the Sutherland Agreement to support its revenue management program. Approval of the recommended actions will allow the Director, or his designee, to execute amendments to the aforementioned Agreements, substantially similar to Exhibits I, II, and III, to extend the term of all three and ensure the continued support of contractors to maximize revenue collection through clearinghouse, billing, and recovery services. The Sutherland and USCB Agreements expire on May 31, 2016, and the Nemadji Agreement expires on August 31, 2016.

The Board previously approved extensions to all three agreements to provide DHS with time to assess its long-term options for organizing and managing its revenue management operations, including the development, release, and evaluation of the necessary solicitations to replace the services provided under the current agreements. DHS also engaged Health Management Associates (HMA) in 2014 to provide specific recommendations related to DHS' revenue cycle operations and procurement strategies for outsourced services.

The HMA report recommended that DHS break out the clearinghouse/Electronic Data Interchange (EDI) function from the Sutherland agreement as it clearly stands on its own. A Request for Proposals (RFP) for a single solution is currently being drafted. HMA also recommended reconfiguring the scope of services under the Sutherland agreement to specifically incorporate data management support and rapid resolution of workload "spikes". Further, HMA recommended clearly delineating the scope of other revenue management program services and concentrate these within two distinct contracts: specifically one for program eligibility determination and subsequent actions and one for recoveries/collections. Last year, the Board subsequently approved an amendment to the FMS, FBRS, and FTPSNRS Agreements to extend the term for an additional year and add clarifying language to each agreement to further enhance security requirements for transmitted data. At that time it was expected that DHS could finish the Clearinghouse/EDI RFP and return to the Board for approval of a successor agreement, as well as do a staggered release of the other RFPs during that time.

Development of RFPs for these distinct contracts has taken longer than initially anticipated. Timelines and DHS staff resources have been impacted during the last two years due to implementation of the Affordable Care Act, implementation of the DHS Electronic Health Record system known as the Online Realtime Centralized Health Information Database (ORCHID), and creation of the Health Agency. It is expected that DHS will make significant progress with the necessary contracting activities during the recommended agreement term extensions.

Implementation of Strategic Plan Goals

The recommendations support Goal 1, Operational Effectiveness/Fiscal Sustainability, of the County's Strategic Plan.

FISCAL IMPACT/FINANCING

Sutherland, USCB, and Nemadji enable DHS and DPH to maximize its revenue collection efforts. During the one-year extension period, DHS estimates that the combined revenue generated by the three contractors will total $1,007,095,969 (Sutherland, $957,867,346; USCB, $35,659,918 and Nemadji, $13,568,705) at a total contract cost of $17,905,100 (Sutherland $13,453,000, USCB, $1,306,150 and Nemadji, $3,145,950), thereby yielding a combined net revenue of $989,206,868 for DHS. DPH estimates $580,000 in revenue from Sutherland at a total contract cost of $285,000 resulting in $295,000 in net revenue for DPH. These contractors receive a fee based on actual revenue collected, which shall remain unchanged during the extension period.

Funding is included in the DHS Fiscal Year (FY) 2015-16 Final Budget and FY 2016-17 Recommended Budget and will be requested in future years as needed.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

Under the current Agreements, Sutherland provides clearinghouse, EDI, billing, revenue recovery, and other financial management services. USCB identifies third-party payers and provides billing services for health care rendered to DHS patients. Nemadji assists DHS in resolving or appealing denied third party coverage claims and recovering revenue from unpaid claims as a last resort after the efforts of DHS and other contractors have been exhausted.

The Amendments restate certain terms and conditions, including revised provisions to further secure and protect the Personally Identifiable Information and Protected Health Information in accordance with the Chief Information Office's directions, as well as updated terminology used in reference to Contractor Self Audits.

The Sutherland Agreement permits the County to terminate the Agreement with or without cause, in whole or in part, with 90-days' prior written notice, while the USCB and Nemadji Agreements allow either party to terminate the Agreement, with or without cause, with 30-days' prior written notice.

County Counsel has approved Exhibits I, II and III as to form.

CONTRACTING PROCESS

During the one-year extension period, DHS anticipates the release of the remaining RFPs for billing and recovery services, and will recommend Board approval of new FMS, FBRS, and FTPSNRS Agreements during the extension period.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommendations will ensure the continued and uninterrupted provision of the revenue management programs and maximize DHS' revenue recovery while DHS completes its RFP process.

Respectfully submitted,

Mitchell H. Katz, M.D.

Director

MHK:adb

Enclosures

c: Chief Executive Office
County Counsel
Executive Office, Board of Supervisors
Interim Director, Department of Public Health

Exhibit I

Agreement No.: H-703466

FINANCIAL MANAGEMENT SERVICES AGREEMENT
AMENDMENT NO. 9

THIS AMENDMENT is made and entered into this _____ day of _____, 2016,

By and between — COUNTY OF LOS ANGELES (hereafter "County"),

And — SUTHERLAND HEALTHCARE SOLUTIONS, INC. (hereafter "Contractor")

Business Address:

9841 Airport Blvd., Suite 1414
Los Angeles, CA 90045

WHEREAS, reference is made to that certain document entitled "FINANCIAL MANAGEMENT SERVICES AGREEMENT", dated September 1, 2008, and further identified as Agreement No. H-703466, and any amendments thereto (all hereafter referred to as "Agreement"); and

WHEREAS, it is the intent of the parties hereto to amend the Agreement to extend the term and to provide for the other changes set forth herein; and

WHEREAS, Agreement provides that changes in accordance to Paragraph 16, Alteration of Terms, may be made in the form of an Amendment which is formally approved and executed by both parties; and

WHEREAS, Contractor warrants that it possesses the competence, expertise and personnel necessary to provide services consistent with the requirements of this Agreement and consistent with the professional standard of care for these services.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. This Amendment shall commence and be effective upon Board approval.

2. Agreement, Paragraph 1, Term, is deleted in its entirety and replaced as follows:

"1. TERM:

The term of this Agreement shall commence September 1, 2008, and shall continue, in full force and effect, through and including June 30, 2017 ("Term").

The County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether the County will exercise a contract term extension option.

The Contractor shall notify DHS when this Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, the Contractor shall send written notification to the DHS at the address provided in Paragraph 18, Notices, of the Agreement."

3. Agreement is modified to add to Additional Provisions, Paragraph 53, Survival:

"53. SURVIVAL: In addition to any provisions of this Agreement which specifically state that they will survive the termination or expiration of this Agreement and any rights and obligations under this Agreement which by their nature should survive, the following Paragraphs shall survive any termination or expiration of this Agreement:

Agreement, Paragraph 6 (Contractor's Close-Out Obligations)

Agreement, Paragraph 7 (No Payment for Services Provided Following Expiration/Termination of Agreement)

Agreement, Paragraph 8 (Indemnification)

Agreement, Paragraph 9 (General Provisions for all Insurance Coverage)

Agreement, Paragraph 10 (Insurance Coverage)

Additional Provisions, Paragraph 8 (Rules and Regulations)

Additional Provisions, Paragraph 15 (Record Retention and Inspection/Audit Settlement)

Additional Provisions, Paragraph 17 (Confidentiality)

Additional Provisions, Paragraph 44 (Governing Law, Jurisdiction, and Venue)

Additional Provisions, Paragraph 53 (Survival)

Exhibit B – Business Associate Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

4. Agreement, Exhibit C-1, Information Security and Privacy Requirements, is deleted and replaced in its entirety by Exhibit C-2, Information Security and Privacy Requirements, attached hereto and incorporated herein by reference. All references to Exhibit C-1 in the Agreement shall hereafter be replaced by Exhibit C-2.

5. Except for the changes set forth hereinabove, Agreement shall not be changed in any respect by this Amendment.

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be executed by the County's Director of Health Services and Contractor has caused this Amendment to be executed on its behalf by its duly authorized officer, the day, month and year first above written.

COUNTY OF LOS ANGELES

By:_____
Mitchell H. Katz, M.D.
Director of Health Services

CONTRACTOR

SUTHERLAND HEALTHCARE SOLUTIONS, INC._____

By: _____
Signature

_____
Printed Name

_____
Title

APPROVED AS TO FORM:
MARY C. WICKHAM
County Counsel

By: _____
Deputy County Counsel

Exhibit C-2

Information Security and Privacy Requirements

to the

Financial Management Services Agreement

EXHIBIT C-2

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

This Exhibit C-2 (Information Security And Privacy Requirements) is an attachment and addition to the Financial Management Services Agreement dated September 1, 2008 (the "**Agreement**") entered into by and between the County of Los Angeles ("**County**") and Sutherland Healthcare Solutions, Inc. ("**Contractor**") and is incorporated into the Agreement by reference hereof. This Exhibit C-2 (Information Security And Privacy Requirements) sets forth information security procedures to be established by Contractor before the Effective Date of the Agreement and maintained throughout the Term of the Agreement. These procedures are in addition to the requirements of the Agreement and the Business Associate Agreement between the Parties. They present a minimum standard only. However, it is Contractor's sole obligation to: (i) implement appropriate measures to secure its systems and data, including Personally Identifiable Information, Protected Health Information, and County Confidential Information, against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum standards set forth in this Exhibit C-2 (Information Security and Privacy Requirements) will constitute a material, non-curable breach of the Agreement by Contractor, entitling County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Agreement, to immediately terminate the Agreement. Unless specifically defined in this Exhibit, capitalized terms shall have the meanings set forth in the Agreement.

1. **Security Policy**. Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (collectively "**Information Security Policy**"). The Information Security Policy will be communicated to all Contractor personnel and subcontractors in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks.

2. **Personnel and Contractor Protections**. Contractor shall screen and conduct background checks on all Contractor personnel and subcontractors contacting County Confidential Information, including Personally Identifiable Information and Protected Health Information, for potential security risks and require all employees, contractors, and subcontractors to sign an appropriate written confidentiality/non-disclosure agreement. All agreements with third-parties involving access to Contractor's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, controls, and procedures for information systems. Contractor shall supply each of its Contractor personnel and subcontractors with appropriate, ongoing training regarding information security procedures, risks, and threats. Contractor shall have an established set of procedures to ensure Contractor personnel and subcontractors promptly report actual and/or suspected breaches of security.

3. **Removable Media**. Except in the context of Contractor's routine back-ups or as otherwise specifically authorized by County in writing, Contractor shall institute strict physical and logical security controls to prevent transfer of Personally Identifiable Information and Protected Health Information to any form of Removable Media. For purposes of this Exhibit C-2 (Information

Security and Privacy Requirements), "**Removable Media**" means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, digital cameras, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

4. **Storage, Transmission, and Destruction of Personally Identifiable Information and Protected Health Information.** All Personally Identifiable Information and Protected Health Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with HIPAA, as amended and supplemented by the HITECH Act and the California Civil Code section 1798 et seq. Without limiting the generality of the foregoing, Contractor shall encrypt (i.e., National Institute of Standards and Technology (NIST) Special Publication (SP) 800-111 Guide to Storage Encryption Technologies for End User Devices[1]) all Personally Identifiable Information and electronic Protected Health Information (stored and during transmission) in accordance with HIPAA and the HITECH Act, as implemented by the U.S. Department of Health and Human Services. If Personally Identifiable Information and Protected Health Information is no longer required to be retained by Contractor under the Agreement and applicable law, Contractor shall destroy such Personally Identifiable Information and Protected Health Information by: (a) shredding or otherwise destroying paper, film, or other hard copy media so that the Personally Identifiable Information and Protected Health Information cannot be read or otherwise cannot be reconstructed; and (b) clearing, purging, or destroying electronic media containing Personally Identifiable Information and Protected Health Information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization[2] and US Department of Defense (DOD) 5220.22-M data sanitization and clearing directive[3] such that the Personally Identifiable Information and Protected Health Information cannot be retrieved.

5. **Data Control; Media Disposal and Servicing**. Subject to and without limiting the requirements under Section 4 (Storage, Transmission and Destruction of Protected Health Information), Personally Identifiable Information, Protected Health Information, and County Confidential Information: (i) may only be made available and accessible to those parties explicitly authorized under the Agreement or otherwise expressly Approved by County in writing; (ii) if transferred across the Internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using industry standard encryption technology in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Guidelines for the Selection and use of Transport Layer Security Implementations[4]; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier or protected using industry standard encryption technology in accordance with NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices[5]. The foregoing requirements shall apply to back-up data stored by Contractor at off-site facilities. In the event any hardware, storage media, or Removable Media must be disposed of or sent off-site for servicing, Contractor shall ensure all County Confidential Information, including Personally Identifiable Information and Protected Health Information, has been cleared, purged, or

[1] Available at http://www.csrc.nist.gov/
[2] Available at http://www.csrc.nist.gov/
[3] Available at http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf
[4] Available at http://www.csrc.nist.gov/
[5] Available at http://www.csrc.nist.gov/

scrubbed from such hardware and/or media using industry best practices in accordance with NIST SP 800-88, Guidelines for Media Sanitization[6]).

6. **Hardware Return**. Upon termination or expiration of the Agreement or at any time upon County's request, Contractor will return all hardware, if any, provided by County containing Personally Identifiable Information, Protected Health Information, or County Confidential Information to County. The Personally Identifiable Information, Protected Health Information, and County Confidential Information shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County. In the event the hardware containing County Confidential Information or Personally Identifiable Information is owned by Contractor or a third-party, a notarized statement, detailing the destruction method used and the data sets involved, the date of destruction, and the company or individual who performed the destruction will be sent to a designated County security representative within fifteen (15) days of termination or expiration of the Agreement or at any time upon County's request. Contractor's destruction or erasure of Personal Information and Protected Health Information pursuant to this Section shall be in compliance with industry Best Practices (e.g., NIST SP 800-88, Guidelines for Media Sanitization[7]).

7. **Physical and Environmental Security**. Contractor facilities that process Personally Identifiable Information, Protected Health Information, or County Confidential Information will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

8. **Communications and Operational Management**. Contractor shall: (i) monitor and manage all of its information processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures; and (ii) deploy adequate anti-viral software and adequate back-up facilities to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures will be adequately documented and designed to protect information, computer media, and data from theft and unauthorized access.

9. **Access Control**. Contractor shall implement formal procedures to control access to its systems, services, and data, including, but not limited to, user account management procedures and the following controls:

   a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of properly configured firewalls;

   b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, authentication, authorization, and event logging;

   c. Applications will include access control to limit user access to information and application system functions; and

[6] Available at http://www.csrc.nist.gov/
[7] Available at http://www.csrc.nist.gov/

d. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with incident response policies set forth below.

10. **Security Incident.** A "Security Incident" shall have the meaning given to such term in 45 C.F.R. § 164.304.

a. Contractor will promptly notify (but in no event more than twenty-four (24) hours after the detection of a Security Incident) the designated County security contact by telephone and subsequently via written letter of any potential or actual security attacks or Security Incidents.

b. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. A Security Incident includes instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately.

c. Contractor will provide a monthly report of all Security Incidents noting the actions taken. This will be provided via a written letter to the County security representative on or before the first (1st) week of each calendar month. County or its third-party designee may, but is not obligated, perform audits and security tests of Contractor's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Personally Identifiable Information, Protected Health Information, and County Confidential Information.

d. In the event County desires to conduct an unannounced penetration test, County shall provide contemporaneous notice to Contractor's Vice President of Audit, or such equivalent position. Any of County's regulators shall have the same right upon request. Contractor shall provide all information reasonably requested by County in connection with any such audits and shall provide reasonable access and assistance to County or its regulators upon request. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes. County reserves the right to view, upon request, any original security reports that Contractor has undertaken on its behalf to assess Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to the County security contact. Contractor will notify County of any new assessments.

11. **Contractor Self Audit.** Contractor will provide to County a summary of: (1) the results of any security audits, security reviews, or other relevant audits listed below, conducted by Contractor or a third-party as applicable; and (2) the corrective actions or modifications, if any, Contractor will implement in response to such audits.

Relevant audits conducted by Contractor as of the Effective Date include:

a. ISO 27001:2013 (Information Security Management) or FDA's Quality System Regulation, etc. – Contractor-Wide. A full recertification is conducted every three (3) years with surveillance audits annually.

(i) **External Audit –** Audit conducted by non-Contractor personnel, to assess Contractor's level of compliance to applicable regulations, standards, and contractual requirements.

(ii) **Internal Audit –** Audit conducted by qualified Contractor Personnel (or contracted designee) not responsible for the area of review, of Contractor organizations, operations, processes, and procedures, to assess compliance to and effectiveness of Contractor's Quality System ("**CQS**") in support of applicable regulations, standards, and requirements.

(iii) **Supplier Audit –** Quality audit conducted by qualified Contractor Personnel (or contracted designee) of product and service suppliers contracted by Contractor for internal or Contractor client use.

(iv) **Detailed findings**- are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above and the ISO certificate is published on Contractor's website.

b. SOC 2 Type II – As to the Hosting Services only:

(i) Audit spans a full twelve (12) months of operation and is produced annually to keep it "up-to-date".

(ii) The resulting detailed report is available to County.

Detailed findings are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above.

12. **Security Audits.** In addition to the audits described in Section 11 (Contractor Self Audit), during the Term of this Agreement, County or its third-party designee may annually, or more frequently as agreed in writing by the Parties, request a security audit (e.g., attestation of security controls) of Contractor's data center and systems. The audit will take place at a time mutually agreed to by the Parties, but in no event on a date more than ninety (90) days from the date of the request by County. County's request for security audit will specify the areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not limited to physical controls inspection, process reviews, policy reviews evidence of external and internal vulnerability scans, penetration tests results, evidence of code reviews, and evidence of system configuration and audit log reviews. County shall pay for all third-party costs associated with the audit. It is understood that summary data of the results may filtered to remove the specific information of other Contractor customers such as IP address, server names, etc. Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators shall have the same right upon request, to request an audit as described above. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

13. **Confidentiality**

a. Except as provided in Section 13(b) (Exclusions) below, each Party agrees that all information supplied by one Party and its affiliates and agents (collectively, the "Disclosing Party") to the other ("Receiving Party") including, without limitation, (a) source code, prices, trade secrets, mask works, databases, designs and techniques, models, displays and manuals; (b) any unpublished information concerning research activities and plans, marketing or sales plans, sales forecasts or results of marketing efforts, pricing or pricing strategies, costs, operational techniques, or strategic plans, and unpublished financial information, including information concerning revenues, profits, and profit margins; (c) any information relating to County's customers, patients, business partners, or personnel; (d) Personally Identifiable Information (as defined below); and (e) Protected Health Information, as specified in Exhibit A (Business Associate Agreement), will be deemed confidential and proprietary to the Disclosing Party, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("Confidential Information"). The foregoing definition shall also include any Confidential Information provided by either Party's contractors, subcontractors, agents, or vendors. To be deemed "Confidential Information", trade secrets and mask works must be plainly and prominently marked with restrictive legends.

b. **Exclusions.** Confidential Information will not include any information or material, or any element thereof, whether or not such information or material is Confidential Information for the purposes of this Agreement, to the extent any such information or material, or any element thereof: (a) has previously become or is generally known, unless it has become generally known through a breach of this Agreement or a similar confidentiality or non-disclosure agreement, obligation or duty; (b) was already rightfully known to the Receiving Party prior to being disclosed by or obtained from the Disclosing Party as evidenced by written records kept in the ordinary course of business or by proof of actual use by the Receiving Party, (c) has been or is hereafter rightfully received by the Receiving Party from a third-party (other than the Disclosing Party) without restriction or disclosure and without breach of a duty of confidentiality to the Disclosing Party; or (d) has been independently developed by the Receiving Party without access to Confidential Information of the Disclosing Party. It will be presumed that any Confidential Information in a Receiving Party's possession is not within exceptions (b), (c) or (d) above, and the burden will be upon the Receiving Party to prove otherwise by records and documentation.

c. **Treatment of Confidential Information.** Each Party recognizes the importance of the other Party's Confidential Information. In particular, each Party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither Party would enter into this Agreement without assurance that such information and the value thereof will be protected as provided in this Section 13 (Confidentiality) and elsewhere in this Agreement. Accordingly, each Party agrees as follows: (a) the Receiving Party will hold any and all Confidential Information it obtains in strictest confidence and will use and permit use of Confidential Information solely for the purposes of this Agreement. Without limiting the foregoing, the Receiving Party shall use at least the same degree of care, but no less than reasonable care, to avoid disclosure or use of this Confidential Information as the Receiving Party employs with respect to its own Confidential Information of a like importance; (b) the Receiving Party may disclose or provide access to its responsible employees, agents, and consultants who have a need to know and may make copies of Confidential Information only to

the extent reasonably necessary to carry out its obligations hereunder; and (c) the Receiving Party currently has, and in the future will maintain in effect and enforce, rules and policies to protect against access to or use or disclosure of Confidential Information other than in accordance with this Agreement, including without limitation written instruction to and agreements with employees, agents, or consultants who are bound by an obligation of confidentiality no less restrictive than set forth in this Agreement to ensure that such employees, agents, and consultants protect the confidentiality of Confidential Information, including this Section 13 (Confidentiality) and Exhibit D (Acknowledgement, Confidentiality and Assignment Agreement). The Receiving Party will require its employees, agents, and consultants not to disclose Confidential Information to third-parties, including without limitation customers, subcontractors, or consultants, without the Disclosing Party's prior written consent, will notify the Disclosing Party immediately of any unauthorized disclosure or use, and will cooperate with the Disclosing Party to protect all proprietary rights in and ownership of its Confidential Information.

d. **Non-Exclusive Equitable Remedy.** Each Party acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may allow a Party or third-parties to unfairly compete with the other Party resulting in irreparable harm to such Party, and therefore, that upon any such breach or any threat thereof, each Party will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 13 (Confidentiality) shall constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the non-breaching Party.

e. **Compelled Disclosures.** To the extent required by applicable law or by lawful order or requirement of a court or governmental authority having competent jurisdiction over the Receiving Party, the Receiving Party may disclose Confidential Information in accordance with such law or order or requirement, subject to the following conditions: as soon as possible after becoming aware of such law, order, or requirement and prior to disclosing Confidential Information pursuant thereto, the Receiving Party will so notify the Disclosing Party in writing and, if possible, the Receiving Party will provide the Disclosing Party notice not less than five (5) Business Days prior to the required disclosure. The Receiving Party will use reasonable efforts not to release Confidential Information pending the outcome of any measures taken by the Disclosing Party to contest, otherwise oppose, or seek to limit such disclosure by the Receiving Party and any subsequent disclosure or use of Confidential Information that may result from such disclosure. The Receiving Party will cooperate with and provide assistance to the Disclosing Party regarding such measures. Notwithstanding any such compelled disclosure by the Receiving Party, such compelled disclosure will not otherwise affect the Receiving Party's obligations hereunder with respect to Confidential Information so disclosed.

f. **County Data.** All of the County Confidential Information, data, records, and information of County to which Contractor has access, or otherwise provided to Contractor under this Agreement ("County Data"), shall be and remain the property of County and County shall retain exclusive rights and ownership thereto. The data of County shall not be used by Contractor for any purpose other than as required under this Agreement, nor shall such data or any part of

such data be disclosed, sold, assigned, leased, or otherwise disposed of to third-parties by Contractor or commercially exploited or otherwise used by or on behalf of Contractor, its officers, directors, employees, or agents.

g. **Personally Identifiable Information.** "Personally Identifiable Information" shall mean any information that identifies a person, including, but not limited to, name, address, email address, passwords, account numbers, social security numbers, credit card information, personal financial or healthcare information, personal preferences, demographic data, marketing data, credit data, or any other identification data. For the avoidance of doubt, Personally Identifiable Information shall include, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("U.S.C.") §6801 et seq.), Protected Health Information, and "Personally Identifiable Information" as that term is defined in California Civil Code section 1798.29 and EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data.

i. Personally Identifiable Information. In connection with this Agreement and performance of the services, Contractor may be provided or obtain, from County or otherwise, Personally Identifiable Information pertaining to County's current and prospective personnel, directors and officers, agents, subcontractors, investors, patients, and customers and may need to process such Personally Identifiable Information and/or transfer it, all subject to the restrictions set forth in this Agreement and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

ii. Treatment of Personally Identifiable Information. Without limiting any other warranty or obligations specified in this Agreement, and in particular the confidential provisions of Section 21 (County Confidential Information), during the Term of this Agreement and thereafter in perpetuity, Contractor will not gather, store, log, archive, use, or otherwise retain any Personally Identifiable Information in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any Personally Identifiable Information to any third-party, except as expressly required to perform its obligations in this Agreement or as Contractor may be expressly directed in advance in writing by County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Agreement, (b) County's then current privacy policy (available at https://intranet.ladhs.org/intracommon/public/DhsPolPro/polProSearchAction.cfm?unit=dhsintra&prog=dhsintra&ou=dhsintra), and (c) all applicable local, state, and federal laws and regulations (including, but not limited to, current and future laws and regulations relating to spamming, privacy, confidentiality, data security, and consumer protection).

iii. Retention of Personally Identifiable Information. Contractor will not retain any Personally Identifiable Information for any period longer than necessary for Contractor to fulfill its obligations under this Agreement. As soon as Contractor no longer needs to retain such Personally Identifiable Information in order to perform its duties under this

Agreement, Contractor will promptly return or destroy or erase all originals and copies of such Personally Identifiable Information.

h. **Return of Confidential Information.** On County's written request or upon expiration or termination of this Agreement for any reason, Contractor will promptly: (a) return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County's Confidential Information; (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Agreement; and (c) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 13(a), and provide a notarized written statement to County certifying that all documents and materials referred to in Subsections 13(a) and (b) have been delivered to County or destroyed, as requested by County. On termination or expiration of this Agreement, County shall return or destroy all Contractor Confidential Information (excluding items licensed to County hereunder or that are required for use of the Deliverables and/or the Licensed Software), at Contractor's option.

Exhibit II

Agreement No.: H-702058

FINANCIAL BILLING AND RECOVERY SERVICES AGREEMENT
AMENDMENT NO. 8

THIS AMENDMENT is made and entered into this _____ day of _____, 2016,

By and between COUNTY OF LOS ANGELES
(hereafter "County"),

And USCB, INC.
(hereafter "Contractor")

Business Address:

3333 Wilshire Blvd., 7th Floor
Los Angeles, CA 90010

WHEREAS, reference is made to that certain document entitled "FINANCIAL BILLING AND RECOVERY SERVICES AGREEMENT", dated July 1, 2006, and further identified as Agreement No. H-702058, and any amendments thereto (all hereafter referred to as "Agreement"); and

WHEREAS, it is the intent of the parties hereto to amend the Agreement to extend the term and to provide for the other changes set forth herein; and

WHEREAS, Agreement provides that changes in accordance to Paragraph 14, Amendments, may be made in the form of an Amendment which is formally approved and executed by both parties; and

WHEREAS, Contractor warrants that it possesses the competence, expertise and personnel necessary to provide services consistent with the requirements of this Agreement and consistent with the professional standard of care for these services.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. This Amendment shall commence and be effective upon Board approval.

2. Agreement, Paragraph 1, Term, is deleted in its entirety and replaced as follows:

"1. TERM: The term of this Agreement shall commence on July 1, 2006, and shall continue, in full force and effect, through and including June 30, 2017 ("Term").

In any event, this Agreement may be canceled or terminated at any time by either party, with or without cause, upon the giving of at least thirty (30) calendar days advance written notice to the other party. Further, County may also suspend the performance of services hereunder, in whole or in part, upon the giving of at least thirty (30) calendar days advance written notice to Contractor. County's notice shall set forth the extent of the suspension and the requirements for full restoration of the performance obligations.

Notwithstanding any other provision of this Agreement, the failure of Contractor or its officers, employees, agents, or subcontractors to comply with any of the terms of this Agreement or any written directions by or on behalf of County issued pursuant hereto shall constitute a material breach hereto, and this Agreement may be terminated by County immediately. County's failure to exercise this right of termination shall not constitute a waiver of such right, which may be exercised at any subsequent time.

The County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether the County will exercise a contract term extension option.

The Contractor shall notify DHS when this Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, the Contractor shall send written notification to the DHS at the address provided in Paragraph 16, Notices, of the Agreement."

3. Agreement is modified to add to Additional Provisions, Paragraph 39, Contractor's Close-Out Obligations, as follows:

"39. CONTRACTOR'S CLOSE-OUT OBLIGATIONS: Contractor shall continue to process all accepted accounts in Contractor's inventory that have been referred to Contractor prior to the time of expiration of this Agreement, unless the Agreement is sooner terminated with or without cause by County. Contractor shall complete the processing of all such accounts and make every effort to expedite

close-out. Contractor shall complete the processing of all such accepted accounts in accordance with the terms and conditions of this Agreement, as well as all required reports."

4. Agreement is modified to add to Additional Provisions, Paragraph 40, No Payment for Services Provided Following Expiration/Termination of Agreement, as follows:

"40. NO PAYMENT FOR SERVICES PROVIDED FOLLOWING EXPIRATION/TERMINATION OF AGREEMENT: The Contractor shall have no claim against the County for payment of any money or reimbursement, of any kind whatsoever, for any service provided by the Contractor after the expiration or other termination of this Agreement. Should the Contractor receive any such payment it shall immediately notify the County and shall immediately repay all such funds to the County. Payment by the County for services rendered after expiration/termination of this Agreement shall not constitute a waiver of the County's right to recover such payment from the Contractor. This provision shall survive the expiration or other termination of this Agreement."

5. Agreement is modified to add to Additional Provisions, Paragraph 41, Survival, as follows:

"41. SURVIVAL: In addition to any provisions of this Agreement which specifically state that they will survive the termination or expiration of this Agreement and any rights and obligations under this Agreement which by their nature should survive, the following Paragraphs shall survive any termination or expiration of this Agreement:

Agreement, Paragraph 5 (Indemnification)

Agreement, Paragraph 6 (General Provisions for all Insurance Coverage)

Agreement, Paragraph 7 (Insurance Coverage)

Agreement, Paragraph 10 (Compliance with Applicable Law)

Additional Provisions, Paragraph 10 (Record Retention and Inspection/Audit Settlement)

Additional Provisions, Paragraph 12 (Confidentiality)

Additional Provisions, Paragraph 30, Sub-paragraph D (Termination

for Convenience)

Additional Provisions, Paragraph 33 (Governing Law, Jurisdiction, and Venue)

Additional Provisions, Paragraph 39, (Contractor's Close-Out Obligations)

Additional Provisions, Paragraph 40, (No Payment for Services Provided Following Expiration/Termination of Agreement)

Additional Provisions, Paragraph 41 (Survival)

Exhibit B – Business Associate Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)"

6. Agreement, Exhibit C-1, Information Security and Privacy Requirements, is deleted and replaced in its entirety by Exhibit C-2, Information Security and Privacy Requirements, attached hereto and incorporated herein by reference. All references to Exhibit C-1 in the Agreement shall hereafter be replaced by Exhibit C-2.

7. Except for the changes set forth hereinabove, Agreement shall not be changed in any respect by this Amendment.

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be executed by the County's Director of Health Services and Contractor has caused this Amendment to be executed on its behalf by its duly authorized officer, the day, month, and year first above written.

COUNTY OF LOS ANGELES

By _____
Mitchell H. Katz, M.D.
Director of Health Services

CONTRACTOR

USCB, INC.

By_____
Signature

_____
Print Name

_____
Title

APPROVED AS TO FORM:
MARY C. WICKHAM
County Counsel

By: _____
Deputy County Counsel

Exhibit C-2

Information Security and Privacy Requirements

to the

Financial Management Services Agreement

EXHIBIT C-2

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

This Exhibit C-2 (Information Security And Privacy Requirements) is an attachment and addition to the Financial Management Services Agreement dated September 1, 2008 (the "**Agreement**") entered into by and between the County of Los Angeles ("**County**") and USCB, Inc. ("**Contractor**") and is incorporated into the Agreement by reference hereof. This Exhibit C-2 (Information Security And Privacy Requirements) sets forth information security procedures to be established by Contractor before the Effective Date of the Agreement and maintained throughout the Term of the Agreement. These procedures are in addition to the requirements of the Agreement and the Business Associate Agreement between the Parties. They present a minimum standard only. However, it is Contractor's sole obligation to: (i) implement appropriate measures to secure its systems and data, including Personally Identifiable Information, Protected Health Information, and County Confidential Information, against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum standards set forth in this Exhibit C-2 (Information Security and Privacy Requirements) will constitute a material, non-curable breach of the Agreement by Contractor, entitling County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Agreement, to immediately terminate the Agreement. Unless specifically defined in this Exhibit, capitalized terms shall have the meanings set forth in the Agreement.

1. **Security Policy**. Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (collectively "**Information Security Policy**"). The Information Security Policy will be communicated to all Contractor personnel and subcontractors in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks.

2. **Personnel and Contractor Protections**. Contractor shall screen and conduct background checks on all Contractor personnel and subcontractors contacting County Confidential Information, including Personally Identifiable Information and Protected Health Information, for potential security risks and require all employees, contractors, and subcontractors to sign an appropriate written confidentiality/non-disclosure agreement. All agreements with third-parties involving access to Contractor's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, controls, and procedures for information systems. Contractor shall supply each of its Contractor personnel and subcontractors with appropriate, ongoing training regarding information security procedures, risks, and threats. Contractor shall have an established set of procedures to ensure Contractor personnel and subcontractors promptly report actual and/or suspected breaches of security.

3. **Removable Media**. Except in the context of Contractor's routine back-ups or as otherwise specifically authorized by County in writing, Contractor shall institute strict physical and logical security controls to prevent transfer of Personally Identifiable Information and Protected Health Information to any form of Removable Media. For purposes of this Exhibit C-2 (Information Security and Privacy Requirements), "**Removable Media**" means portable or removable hard

disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, digital cameras, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

4. **Storage, Transmission, and Destruction of Personally Identifiable Information and Protected Health Information.** All Personally Identifiable Information and Protected Health Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with HIPAA, as amended and supplemented by the HITECH Act and the California Civil Code section 1798 et seq. Without limiting the generality of the foregoing, Contractor shall encrypt (i.e., National Institute of Standards and Technology (NIST) Special Publication (SP) 800-111 Guide to Storage Encryption Technologies for End User Devices[1]) all Personally Identifiable Information and electronic Protected Health Information (stored and during transmission) in accordance with HIPAA and the HITECH Act, as implemented by the U.S. Department of Health and Human Services. If Personally Identifiable Information and Protected Health Information is no longer required to be retained by Contractor under the Agreement and applicable law, Contractor shall destroy such Personally Identifiable Information and Protected Health Information by: (a) shredding or otherwise destroying paper, film, or other hard copy media so that the Personally Identifiable Information and Protected Health Information cannot be read or otherwise cannot be reconstructed; and (b) clearing, purging, or destroying electronic media containing Personally Identifiable Information and Protected Health Information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization[2] and US Department of Defense (DOD) 5220.22-M data sanitization and clearing directive[3] such that the Personally Identifiable Information and Protected Health Information cannot be retrieved.

5. **Data Control; Media Disposal and Servicing**. Subject to and without limiting the requirements under Section 4 (Storage, Transmission and Destruction of Protected Health Information), Personally Identifiable Information, Protected Health Information, and County Confidential Information: (i) may only be made available and accessible to those parties explicitly authorized under the Agreement or otherwise expressly Approved by County in writing; (ii) if transferred across the Internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using industry standard encryption technology in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Guidelines for the Selection and use of Transport Layer Security Implementations[4]; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier or protected using industry standard encryption technology in accordance with NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices[5]. The foregoing requirements shall apply to back-up data stored by Contractor at off-site facilities. In the event any hardware, storage media, or Removable Media must be disposed of or sent off-site for servicing, Contractor shall ensure all County Confidential Information, including Personally Identifiable Information and Protected Health Information, has been cleared, purged, or

[1] Available at http://www.csrc.nist.gov/
[2] Available at http://www.csrc.nist.gov/
[3] Available at http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf
[4] Available at http://www.csrc.nist.gov/
[5] Available at http://www.csrc.nist.gov/

scrubbed from such hardware and/or media using industry best practices in accordance with NIST SP 800-88, Guidelines for Media Sanitization[6]).

6. **Hardware Return**. Upon termination or expiration of the Agreement or at any time upon County's request, Contractor will return all hardware, if any, provided by County containing Personally Identifiable Information, Protected Health Information, or County Confidential Information to County. The Personally Identifiable Information, Protected Health Information, and County Confidential Information shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County. In the event the hardware containing County Confidential Information or Personally Identifiable Information is owned by Contractor or a third-party, a notarized statement, detailing the destruction method used and the data sets involved, the date of destruction, and the company or individual who performed the destruction will be sent to a designated County security representative within fifteen (15) days of termination or expiration of the Agreement or at any time upon County's request. Contractor's destruction or erasure of Personal Information and Protected Health Information pursuant to this Section shall be in compliance with industry Best Practices (e.g., NIST SP 800-88, Guidelines for Media Sanitization[7]).

7. **Physical and Environmental Security**. Contractor facilities that process Personally Identifiable Information, Protected Health Information, or County Confidential Information will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

8. **Communications and Operational Management**. Contractor shall: (i) monitor and manage all of its information processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures; and (ii) deploy adequate anti-viral software and adequate back-up facilities to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures will be adequately documented and designed to protect information, computer media, and data from theft and unauthorized access.

9. **Access Control**. Contractor shall implement formal procedures to control access to its systems, services, and data, including, but not limited to, user account management procedures and the following controls:

   a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of properly configured firewalls;

   b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, authentication, authorization, and event logging;

   c. Applications will include access control to limit user access to information and application system functions; and

[6] Available at http://www.csrc.nist.gov/
[7] Available at http://www.csrc.nist.gov/

d. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with incident response policies set forth below.

10. **Security Incident.** A "Security Incident" shall have the meaning given to such term in 45 C.F.R. § 164.304.

a. Contractor will promptly notify (but in no event more than twenty-four (24) hours after the detection of a Security Incident) the designated County security contact by telephone and subsequently via written letter of any potential or actual security attacks or Security Incidents.

b. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. A Security Incident includes instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately.

c. Contractor will provide a monthly report of all Security Incidents noting the actions taken. This will be provided via a written letter to the County security representative on or before the first (1st) week of each calendar month. County or its third-party designee may, but is not obligated, perform audits and security tests of Contractor's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Personally Identifiable Information, Protected Health Information, and County Confidential Information.

d. In the event County desires to conduct an unannounced penetration test, County shall provide contemporaneous notice to Contractor's Vice President of Audit, or such equivalent position. Any of County's regulators shall have the same right upon request. Contractor shall provide all information reasonably requested by County in connection with any such audits and shall provide reasonable access and assistance to County or its regulators upon request. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes. County reserves the right to view, upon request, any original security reports that Contractor has undertaken on its behalf to assess Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to the County security contact. Contractor will notify County of any new assessments.

11. **Contractor Self Audit.** Contractor will provide to County a summary of: (1) the results of any security audits, security reviews, or other relevant audits listed below, conducted by Contractor or a third-party as applicable; and (2) the corrective actions or modifications, if any, Contractor will implement in response to such audits.

Relevant audits conducted by Contractor as of the Effective Date include:

a. ISO 27001:2013 (Information Security Management) or FDA's Quality System Regulation, etc. – Contractor-Wide. A full recertification is conducted every three (3) years with surveillance audits annually.

(i) **External Audit –** Audit conducted by non-Contractor personnel, to assess Contractor's level of compliance to applicable regulations, standards, and contractual requirements.

(ii) **Internal Audit –** Audit conducted by qualified Contractor Personnel (or contracted designee) not responsible for the area of review, of Contractor organizations, operations, processes, and procedures, to assess compliance to and effectiveness of Contractor's Quality System ("**CQS**") in support of applicable regulations, standards, and requirements.

(iii) **Supplier Audit –** Quality audit conducted by qualified Contractor Personnel (or contracted designee) of product and service suppliers contracted by Contractor for internal or Contractor client use.

(iv) **Detailed findings**- are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above and the ISO certificate is published on Contractor's website.

b. SOC 2 Type II – As to the Hosting Services only:

(i) Audit spans a full twelve (12) months of operation and is produced annually to keep it "up-to-date".

(ii) The resulting detailed report is available to County.

Detailed findings are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above.

12. **Security Audits.** In addition to the audits described in Section 11 (Contractor Self Audit), during the Term of this Agreement, County or its third-party designee may annually, or more frequently as agreed in writing by the Parties, request a security audit (e.g., attestation of security controls) of Contractor's data center and systems. The audit will take place at a time mutually agreed to by the Parties, but in no event on a date more than ninety (90) days from the date of the request by County. County's request for security audit will specify the areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not limited to physical controls inspection, process reviews, policy reviews evidence of external and internal vulnerability scans, penetration tests results, evidence of code reviews, and evidence of system configuration and audit log reviews. County shall pay for all third-party costs associated with the audit. It is understood that summary data of the results may filtered to remove the specific information of other Contractor customers such as IP address, server names, etc. Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators shall have the same right upon request, to request an audit as described above. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

13. **Confidentiality**

a. Except as provided in Section 13(b) (Exclusions) below, each Party agrees that all information supplied by one Party and its affiliates and agents (collectively, the "Disclosing Party") to the other ("Receiving Party") including, without limitation, (a) source code, prices, trade secrets, mask works, databases, designs and techniques, models, displays and manuals; (b) any unpublished information concerning research activities and plans, marketing or sales plans, sales forecasts or results of marketing efforts, pricing or pricing strategies, costs, operational techniques, or strategic plans, and unpublished financial information, including information concerning revenues, profits, and profit margins; (c) any information relating to County's customers, patients, business partners, or personnel; (d) Personally Identifiable Information (as defined below); and (e) Protected Health Information, as specified in Exhibit A (Business Associate Agreement), will be deemed confidential and proprietary to the Disclosing Party, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("Confidential Information"). The foregoing definition shall also include any Confidential Information provided by either Party's contractors, subcontractors, agents, or vendors. To be deemed "Confidential Information", trade secrets and mask works must be plainly and prominently marked with restrictive legends.

b. **Exclusions.** Confidential Information will not include any information or material, or any element thereof, whether or not such information or material is Confidential Information for the purposes of this Agreement, to the extent any such information or material, or any element thereof: (a) has previously become or is generally known, unless it has become generally known through a breach of this Agreement or a similar confidentiality or non-disclosure agreement, obligation or duty; (b) was already rightfully known to the Receiving Party prior to being disclosed by or obtained from the Disclosing Party as evidenced by written records kept in the ordinary course of business or by proof of actual use by the Receiving Party, (c) has been or is hereafter rightfully received by the Receiving Party from a third-party (other than the Disclosing Party) without restriction or disclosure and without breach of a duty of confidentiality to the Disclosing Party; or (d) has been independently developed by the Receiving Party without access to Confidential Information of the Disclosing Party. It will be presumed that any Confidential Information in a Receiving Party's possession is not within exceptions (b), (c) or (d) above, and the burden will be upon the Receiving Party to prove otherwise by records and documentation.

c. **Treatment of Confidential Information.** Each Party recognizes the importance of the other Party's Confidential Information. In particular, each Party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither Party would enter into this Agreement without assurance that such information and the value thereof will be protected as provided in this Section 13 (Confidentiality) and elsewhere in this Agreement. Accordingly, each Party agrees as follows: (a) the Receiving Party will hold any and all Confidential Information it obtains in strictest confidence and will use and permit use of Confidential Information solely for the purposes of this Agreement. Without limiting the foregoing, the Receiving Party shall use at least the same degree of care, but no less than reasonable care, to avoid disclosure or use of this Confidential Information as the Receiving Party employs with respect to its own Confidential Information of a like importance; (b) the Receiving Party may disclose or provide access to its responsible employees, agents, and consultants who have a need to know and may make copies of Confidential Information only to

the extent reasonably necessary to carry out its obligations hereunder; and (c) the Receiving Party currently has, and in the future will maintain in effect and enforce, rules and policies to protect against access to or use or disclosure of Confidential Information other than in accordance with this Agreement, including without limitation written instruction to and agreements with employees, agents, or consultants who are bound by an obligation of confidentiality no less restrictive than set forth in this Agreement to ensure that such employees, agents, and consultants protect the confidentiality of Confidential Information, including this Section 13 (Confidentiality) and Exhibit D (Acknowledgement, Confidentiality and Assignment Agreement). The Receiving Party will require its employees, agents, and consultants not to disclose Confidential Information to third-parties, including without limitation customers, subcontractors, or consultants, without the Disclosing Party's prior written consent, will notify the Disclosing Party immediately of any unauthorized disclosure or use, and will cooperate with the Disclosing Party to protect all proprietary rights in and ownership of its Confidential Information.

d. **Non-Exclusive Equitable Remedy.** Each Party acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may allow a Party or third-parties to unfairly compete with the other Party resulting in irreparable harm to such Party, and therefore, that upon any such breach or any threat thereof, each Party will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 13 (Confidentiality) shall constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the non-breaching Party.

e. **Compelled Disclosures.** To the extent required by applicable law or by lawful order or requirement of a court or governmental authority having competent jurisdiction over the Receiving Party, the Receiving Party may disclose Confidential Information in accordance with such law or order or requirement, subject to the following conditions: as soon as possible after becoming aware of such law, order, or requirement and prior to disclosing Confidential Information pursuant thereto, the Receiving Party will so notify the Disclosing Party in writing and, if possible, the Receiving Party will provide the Disclosing Party notice not less than five (5) Business Days prior to the required disclosure. The Receiving Party will use reasonable efforts not to release Confidential Information pending the outcome of any measures taken by the Disclosing Party to contest, otherwise oppose, or seek to limit such disclosure by the Receiving Party and any subsequent disclosure or use of Confidential Information that may result from such disclosure. The Receiving Party will cooperate with and provide assistance to the Disclosing Party regarding such measures. Notwithstanding any such compelled disclosure by the Receiving Party, such compelled disclosure will not otherwise affect the Receiving Party's obligations hereunder with respect to Confidential Information so disclosed.

f. **County Data.** All of the County Confidential Information, data, records, and information of County to which Contractor has access, or otherwise provided to Contractor under this Agreement ("County Data"), shall be and remain the property of County and County shall retain exclusive rights and ownership thereto. The data of County shall not be used by Contractor for any purpose other than as required under this Agreement, nor shall such data or any part of

such data be disclosed, sold, assigned, leased, or otherwise disposed of to third-parties by Contractor or commercially exploited or otherwise used by or on behalf of Contractor, its officers, directors, employees, or agents.

g. **Personally Identifiable Information.** "Personally Identifiable Information" shall mean any information that identifies a person, including, but not limited to, name, address, email address, passwords, account numbers, social security numbers, credit card information, personal financial or healthcare information, personal preferences, demographic data, marketing data, credit data, or any other identification data. For the avoidance of doubt, Personally Identifiable Information shall include, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("U.S.C.") §6801 et seq.), Protected Health Information, and "Personally Identifiable Information" as that term is defined in California Civil Code section 1798.29 and EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data.

i. Personally Identifiable Information. In connection with this Agreement and performance of the services, Contractor may be provided or obtain, from County or otherwise, Personally Identifiable Information pertaining to County's current and prospective personnel, directors and officers, agents, subcontractors, investors, patients, and customers and may need to process such Personally Identifiable Information and/or transfer it, all subject to the restrictions set forth in this Agreement and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

ii. Treatment of Personally Identifiable Information. Without limiting any other warranty or obligations specified in this Agreement, and in particular the confidential provisions of Section 21 (County Confidential Information), during the Term of this Agreement and thereafter in perpetuity, Contractor will not gather, store, log, archive, use, or otherwise retain any Personally Identifiable Information in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any Personally Identifiable Information to any third-party, except as expressly required to perform its obligations in this Agreement or as Contractor may be expressly directed in advance in writing by County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Agreement, (b) County's then current privacy policy (available at https://intranet.ladhs.org/intracommon/public/DhsPolPro/polProSearchAction.cfm?unit=dhsintra&prog=dhsintra&ou=dhsintra), and (c) all applicable local, state, and federal laws and regulations (including, but not limited to, current and future laws and regulations relating to spamming, privacy, confidentiality, data security, and consumer protection).

iii. Retention of Personally Identifiable Information. Contractor will not retain any Personally Identifiable Information for any period longer than necessary for Contractor to fulfill its obligations under this Agreement. As soon as Contractor no longer needs to retain such Personally Identifiable Information in order to perform its duties under this

Agreement, Contractor will promptly return or destroy or erase all originals and copies of such Personally Identifiable Information.

h. **Return of Confidential Information.** On County's written request or upon expiration or termination of this Agreement for any reason, Contractor will promptly: (a) return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County's Confidential Information; (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Agreement; and (c) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 13(a), and provide a notarized written statement to County certifying that all documents and materials referred to in Subsections 13(a) and (b) have been delivered to County or destroyed, as requested by County. On termination or expiration of this Agreement, County shall return or destroy all Contractor Confidential Information (excluding items licensed to County hereunder or that are required for use of the Deliverables and/or the Licensed Software), at Contractor's option.

Exhibit III

Agreement No.: H-703452

FINAL THIRD PARTY SAFETY NET AND RECOVERY SERVICES AGREEMENT
AMENDMENT NO. 6

THIS AMENDMENT is made and entered into this _____ day of _____, 2016,

By and between COUNTY OF LOS ANGELES
(hereafter "County"),

And NEMADJI RESEARCH CORPORATION
dba CALIFORNIA REIMBURSEMENT ENTERPRISES
(hereafter "Contractor")

Business Address:
P.O. Box 100
7564 Birch Street
Bruno, MN 55712

WHEREAS, reference is made to that certain document entitled "FINAL THIRD PARTY SAFETY NET AND RECOVERY SERVICES AGREEMENT", dated September 1, 2008, and further identified as Agreement No. H-703452, and any amendments thereto (all hereafter referred to as "Agreement") and

WHEREAS, it is the intent of the parties hereto to amend the Agreement to extend the term, and to provide for the other changes set forth herein; and

WHEREAS, Agreement provides that changes in accordance to Paragraph 16, Alteration of Terms, may be made in the form of an Amendment which is formally approved and executed by both parties.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. This Amendment shall commence and be effective upon Board approval.

2. Agreement, Paragraph 1, Term, is deleted in its entirety and replaced as follows:

"1. TERM:

The term of this Agreement shall commence September 1, 2008, and shall continue, in full force and effect, through and including August 31, 2017 (“Term”).

In any event, this Agreement may be canceled or terminated at any time by either party, with or without cause, upon the giving of at least thirty (30) days' prior written notice to the other.

Notwithstanding any other provision of this Paragraph, the failure of Contractor or its officers, employees, agents, or subcontractors, to comply with any of the terms of this Agreement or any written directions by or on behalf of County issued pursuant hereto shall constitute a material breach hereto, and this Agreement may be terminated by County immediately. County's failure to exercise this right of termination shall not constitute a waiver of such right, which may be exercised at any subsequent time.

The County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether the County will exercise a contract term extension option.

The Contractor shall notify DHS when this Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, the Contractor shall send written notification to the DHS at the address provided in Paragraph 18, NOTICES, of the Agreement."

3. Agreement is modified to add to Additional Provisions, Paragraph 39, Survival, as follows:

"39. SURVIVAL: In addition to any provisions of this Agreement which specifically state that they will survive the termination or expiration of this Agreement and any rights and obligations under this Agreement which by their nature should survive, the following Paragraphs shall survive any termination or expiration of this Agreement:

Agreement, Paragraph 6 (Contractor's Close-Out Obligations)

Agreement, Paragraph 7 (No Payment for Services Provided Following Expiration/Termination of Agreement)

Agreement, Paragraph 8 (Indemnification)

Agreement, Paragraph 9 (General Provisions for all Insurance Coverage)

Agreement, Paragraph 10 (Insurance Coverage)

Additional Provisions, Paragraph 8 (Rules and Regulations)

Additional Provisions, Paragraph 15 (Record Retention and Inspection/Audit Settlement)

Additional Provisions, Paragraph 17 (Confidentiality)

Additional Provisions, Paragraph 44 (Governing Law, Jurisdiction, and Venue)

Additional Provisions, Paragraph 53 (Survival)

Exhibit B – Business Associate Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)"

4. Agreement, Exhibit C-1, Information Security and Privacy Requirements, is deleted and replaced in its entirety by Exhibit C-2, Information Security and Privacy Requirements, attached hereto and incorporated herein by reference. All references to Exhibit C-1 in the Agreement shall hereafter be replaced by Exhibit C-2.

5. Except for the changes set forth hereinabove, Agreement shall not be changed in any respect by this Amendment.

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be executed by the County's Director of Health Services and Contractor has caused this Amendment to be executed on its behalf by its duly authorized officer, the day, month and year first above written.

COUNTY OF LOS ANGELES

By _____
Mitchell H. Katz, M.D.
Director of Health Services

CONTRACTOR

NEMADJI RESEARCH CORPORATION
dba CALIFORNIA REIMBURSEMENT
ENTERPRISES

By: _____
Signature

_____
Printed Name

_____
Title

APPROVED AS TO FORM:
MARY C. WICKHAM
County Counsel

By:_____
Deputy County Counsel

Exhibit C-2

Information Security and Privacy Requirements

to the

Financial Management Services Agreement

EXHIBIT C-2

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

This Exhibit C-2 (Information Security And Privacy Requirements) is an attachment and addition to the Financial Management Services Agreement dated September 1, 2008 (the "**Agreement**") entered into by and between the County of Los Angeles ("**County**") and Nemadji Research Corporation dba California Reimbursement Corporation ("**Contractor**") and is incorporated into the Agreement by reference hereof. This Exhibit C-2 (Information Security And Privacy Requirements) sets forth information security procedures to be established by Contractor before the Effective Date of the Agreement and maintained throughout the Term of the Agreement. These procedures are in addition to the requirements of the Agreement and the Business Associate Agreement between the Parties. They present a minimum standard only. However, it is Contractor's sole obligation to: (i) implement appropriate measures to secure its systems and data, including Personally Identifiable Information, Protected Health Information, and County Confidential Information, against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum standards set forth in this Exhibit C-2 (Information Security and Privacy Requirements) will constitute a material, non-curable breach of the Agreement by Contractor, entitling County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Agreement, to immediately terminate the Agreement. Unless specifically defined in this Exhibit, capitalized terms shall have the meanings set forth in the Agreement.

1. **Security Policy**. Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (collectively "**Information Security Policy**"). The Information Security Policy will be communicated to all Contractor personnel and subcontractors in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks.

2. **Personnel and Contractor Protections**. Contractor shall screen and conduct background checks on all Contractor personnel and subcontractors contacting County Confidential Information, including Personally Identifiable Information and Protected Health Information, for potential security risks and require all employees, contractors, and subcontractors to sign an appropriate written confidentiality/non-disclosure agreement. All agreements with third-parties involving access to Contractor's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, controls, and procedures for information systems. Contractor shall supply each of its Contractor personnel and subcontractors with appropriate, ongoing training regarding information security procedures, risks, and threats. Contractor shall have an established set of procedures to ensure Contractor personnel and subcontractors promptly report actual and/or suspected breaches of security.

3. **Removable Media**. Except in the context of Contractor's routine back-ups or as otherwise specifically authorized by County in writing, Contractor shall institute strict physical and logical security controls to prevent transfer of Personally Identifiable Information and Protected Health Information to any form of Removable Media. For purposes of this Exhibit C-2 (Information

Security and Privacy Requirements), "**Removable Media**" means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, digital cameras, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

4. **Storage, Transmission, and Destruction of Personally Identifiable Information and Protected Health Information.** All Personally Identifiable Information and Protected Health Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with HIPAA, as amended and supplemented by the HITECH Act and the California Civil Code section 1798 et seq. Without limiting the generality of the foregoing, Contractor shall encrypt (i.e., National Institute of Standards and Technology (NIST) Special Publication (SP) 800-111 Guide to Storage Encryption Technologies for End User Devices[1]) all Personally Identifiable Information and electronic Protected Health Information (stored and during transmission) in accordance with HIPAA and the HITECH Act, as implemented by the U.S. Department of Health and Human Services. If Personally Identifiable Information and Protected Health Information is no longer required to be retained by Contractor under the Agreement and applicable law, Contractor shall destroy such Personally Identifiable Information and Protected Health Information by: (a) shredding or otherwise destroying paper, film, or other hard copy media so that the Personally Identifiable Information and Protected Health Information cannot be read or otherwise cannot be reconstructed; and (b) clearing, purging, or destroying electronic media containing Personally Identifiable Information and Protected Health Information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization[2] and US Department of Defense (DOD) 5220.22-M data sanitization and clearing directive[3] such that the Personally Identifiable Information and Protected Health Information cannot be retrieved.

5. **Data Control; Media Disposal and Servicing**. Subject to and without limiting the requirements under Section 4 (Storage, Transmission and Destruction of Protected Health Information), Personally Identifiable Information, Protected Health Information, and County Confidential Information: (i) may only be made available and accessible to those parties explicitly authorized under the Agreement or otherwise expressly Approved by County in writing; (ii) if transferred across the Internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using industry standard encryption technology in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Guidelines for the Selection and use of Transport Layer Security Implementations[4]; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier or protected using industry standard encryption technology in accordance with NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices[5]. The foregoing requirements shall apply to back-up data stored by Contractor at off-site facilities. In the event any hardware, storage media, or Removable Media must be disposed of or sent off-site for servicing, Contractor shall ensure all County Confidential Information, including Personally Identifiable Information and Protected Health Information, has been cleared, purged, or

[1] Available at http://www.csrc.nist.gov/
[2] Available at http://www.csrc.nist.gov/
[3] Available at http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf
[4] Available at http://www.csrc.nist.gov/
[5] Available at http://www.csrc.nist.gov/

scrubbed from such hardware and/or media using industry best practices in accordance with NIST SP 800-88, Guidelines for Media Sanitization[6]).

6. **Hardware Return**. Upon termination or expiration of the Agreement or at any time upon County's request, Contractor will return all hardware, if any, provided by County containing Personally Identifiable Information, Protected Health Information, or County Confidential Information to County. The Personally Identifiable Information, Protected Health Information, and County Confidential Information shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County. In the event the hardware containing County Confidential Information or Personally Identifiable Information is owned by Contractor or a third-party, a notarized statement, detailing the destruction method used and the data sets involved, the date of destruction, and the company or individual who performed the destruction will be sent to a designated County security representative within fifteen (15) days of termination or expiration of the Agreement or at any time upon County's request. Contractor's destruction or erasure of Personal Information and Protected Health Information pursuant to this Section shall be in compliance with industry Best Practices (e.g., NIST SP 800-88, Guidelines for Media Sanitization[7]).

7. **Physical and Environmental Security**. Contractor facilities that process Personally Identifiable Information, Protected Health Information, or County Confidential Information will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

8. **Communications and Operational Management**. Contractor shall: (i) monitor and manage all of its information processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures; and (ii) deploy adequate anti-viral software and adequate back-up facilities to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures will be adequately documented and designed to protect information, computer media, and data from theft and unauthorized access.

9. **Access Control**. Contractor shall implement formal procedures to control access to its systems, services, and data, including, but not limited to, user account management procedures and the following controls:

   a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of properly configured firewalls;

   b. Operating systems will be used to enforce access controls to computer resources including, but not limited to, authentication, authorization, and event logging;

   c. Applications will include access control to limit user access to information and application system functions; and

[6] Available at http://www.csrc.nist.gov/
[7] Available at http://www.csrc.nist.gov/

d. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with incident response policies set forth below.

10. **Security Incident.** A "Security Incident" shall have the meaning given to such term in 45 C.F.R. § 164.304.

a. Contractor will promptly notify (but in no event more than twenty-four (24) hours after the detection of a Security Incident) the designated County security contact by telephone and subsequently via written letter of any potential or actual security attacks or Security Incidents.

b. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. A Security Incident includes instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately.

c. Contractor will provide a monthly report of all Security Incidents noting the actions taken. This will be provided via a written letter to the County security representative on or before the first (1st) week of each calendar month. County or its third-party designee may, but is not obligated, perform audits and security tests of Contractor's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Personally Identifiable Information, Protected Health Information, and County Confidential Information.

d. In the event County desires to conduct an unannounced penetration test, County shall provide contemporaneous notice to Contractor's Vice President of Audit, or such equivalent position. Any of County's regulators shall have the same right upon request. Contractor shall provide all information reasonably requested by County in connection with any such audits and shall provide reasonable access and assistance to County or its regulators upon request. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes. County reserves the right to view, upon request, any original security reports that Contractor has undertaken on its behalf to assess Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to the County security contact. Contractor will notify County of any new assessments.

11. **Contractor Self Audit.** Contractor will provide to County a summary of: (1) the results of any security audits, security reviews, or other relevant audits listed below, conducted by Contractor or a third-party as applicable; and (2) the corrective actions or modifications, if any, Contractor will implement in response to such audits.

Relevant audits conducted by Contractor as of the Effective Date include:

a. ISO 27001:2013 (Information Security Management) or FDA's Quality System Regulation, etc. – Contractor-Wide. A full recertification is conducted every three (3) years with surveillance audits annually.

(i) **External Audit –** Audit conducted by non-Contractor personnel, to assess Contractor's level of compliance to applicable regulations, standards, and contractual requirements.

(ii) **Internal Audit –** Audit conducted by qualified Contractor Personnel (or contracted designee) not responsible for the area of review, of Contractor organizations, operations, processes, and procedures, to assess compliance to and effectiveness of Contractor's Quality System ("**CQS**") in support of applicable regulations, standards, and requirements.

(iii) **Supplier Audit –** Quality audit conducted by qualified Contractor Personnel (or contracted designee) of product and service suppliers contracted by Contractor for internal or Contractor client use.

(iv) **Detailed findings**- are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above and the ISO certificate is published on Contractor's website.

b. SOC 2 Type II Report – As to the Hosting Services only:

(i) Audit spans a full twelve (12) months of operation and is produced annually to keep it "up-to-date".

(ii) The resulting detailed report is available to County.

Detailed findings are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above.

12. **Security Audits.** In addition to the audits described in Section 11 (Contractor Self Audit), during the Term of this Agreement, County or its third-party designee may annually, or more frequently as agreed in writing by the Parties, request a security audit (e.g., attestation of security controls) of Contractor's data center and systems. The audit will take place at a time mutually agreed to by the Parties, but in no event on a date more than ninety (90) days from the date of the request by County. County's request for security audit will specify the areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not limited to physical controls inspection, process reviews, policy reviews evidence of external and internal vulnerability scans, penetration tests results, evidence of code reviews, and evidence of system configuration and audit log reviews. County shall pay for all third-party costs associated with the audit. It is understood that summary data of the results may filtered to remove the specific information of other Contractor customers such as IP address, server names, etc. Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators shall have the same right upon request, to request an audit as described above. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

13. **Confidentiality**

a. Except as provided in Section 13(b) (Exclusions) below, each Party agrees that all information supplied by one Party and its affiliates and agents (collectively, the "Disclosing Party") to the other ("Receiving Party") including, without limitation, (a) source code, prices, trade secrets, mask works, databases, designs and techniques, models, displays and manuals; (b) any unpublished information concerning research activities and plans, marketing or sales plans, sales forecasts or results of marketing efforts, pricing or pricing strategies, costs, operational techniques, or strategic plans, and unpublished financial information, including information concerning revenues, profits, and profit margins; (c) any information relating to County's customers, patients, business partners, or personnel; (d) Personally Identifiable Information (as defined below); and (e) Protected Health Information, as specified in Exhibit A (Business Associate Agreement), will be deemed confidential and proprietary to the Disclosing Party, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("Confidential Information"). The foregoing definition shall also include any Confidential Information provided by either Party's contractors, subcontractors, agents, or vendors. To be deemed "Confidential Information", trade secrets and mask works must be plainly and prominently marked with restrictive legends.

b. **Exclusions.** Confidential Information will not include any information or material, or any element thereof, whether or not such information or material is Confidential Information for the purposes of this Agreement, to the extent any such information or material, or any element thereof: (a) has previously become or is generally known, unless it has become generally known through a breach of this Agreement or a similar confidentiality or non-disclosure agreement, obligation or duty; (b) was already rightfully known to the Receiving Party prior to being disclosed by or obtained from the Disclosing Party as evidenced by written records kept in the ordinary course of business or by proof of actual use by the Receiving Party, (c) has been or is hereafter rightfully received by the Receiving Party from a third-party (other than the Disclosing Party) without restriction or disclosure and without breach of a duty of confidentiality to the Disclosing Party; or (d) has been independently developed by the Receiving Party without access to Confidential Information of the Disclosing Party. It will be presumed that any Confidential Information in a Receiving Party's possession is not within exceptions (b), (c) or (d) above, and the burden will be upon the Receiving Party to prove otherwise by records and documentation.

c. **Treatment of Confidential Information.** Each Party recognizes the importance of the other Party's Confidential Information. In particular, each Party recognizes and agrees that the Confidential Information of the other is critical to their respective businesses and that neither Party would enter into this Agreement without assurance that such information and the value thereof will be protected as provided in this Section 13 (Confidentiality) and elsewhere in this Agreement. Accordingly, each Party agrees as follows: (a) the Receiving Party will hold any and all Confidential Information it obtains in strictest confidence and will use and permit use of Confidential Information solely for the purposes of this Agreement. Without limiting the foregoing, the Receiving Party shall use at least the same degree of care, but no less than reasonable care, to avoid disclosure or use of this Confidential Information as the Receiving Party employs with respect to its own Confidential Information of a like importance; (b) the Receiving Party may disclose or provide access to its responsible employees, agents, and consultants who have a need to know and may make copies of Confidential Information only to

the extent reasonably necessary to carry out its obligations hereunder; and (c) the Receiving Party currently has, and in the future will maintain in effect and enforce, rules and policies to protect against access to or use or disclosure of Confidential Information other than in accordance with this Agreement, including without limitation written instruction to and agreements with employees, agents, or consultants who are bound by an obligation of confidentiality no less restrictive than set forth in this Agreement to ensure that such employees, agents, and consultants protect the confidentiality of Confidential Information, including this Section 13 (Confidentiality) and Exhibit D (Acknowledgement, Confidentiality and Assignment Agreement). The Receiving Party will require its employees, agents, and consultants not to disclose Confidential Information to third-parties, including without limitation customers, subcontractors, or consultants, without the Disclosing Party's prior written consent, will notify the Disclosing Party immediately of any unauthorized disclosure or use, and will cooperate with the Disclosing Party to protect all proprietary rights in and ownership of its Confidential Information.

d. **Non-Exclusive Equitable Remedy.** Each Party acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may allow a Party or third-parties to unfairly compete with the other Party resulting in irreparable harm to such Party, and therefore, that upon any such breach or any threat thereof, each Party will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 13 (Confidentiality) shall constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the non-breaching Party.

e. **Compelled Disclosures.** To the extent required by applicable law or by lawful order or requirement of a court or governmental authority having competent jurisdiction over the Receiving Party, the Receiving Party may disclose Confidential Information in accordance with such law or order or requirement, subject to the following conditions: as soon as possible after becoming aware of such law, order, or requirement and prior to disclosing Confidential Information pursuant thereto, the Receiving Party will so notify the Disclosing Party in writing and, if possible, the Receiving Party will provide the Disclosing Party notice not less than five (5) Business Days prior to the required disclosure. The Receiving Party will use reasonable efforts not to release Confidential Information pending the outcome of any measures taken by the Disclosing Party to contest, otherwise oppose, or seek to limit such disclosure by the Receiving Party and any subsequent disclosure or use of Confidential Information that may result from such disclosure. The Receiving Party will cooperate with and provide assistance to the Disclosing Party regarding such measures. Notwithstanding any such compelled disclosure by the Receiving Party, such compelled disclosure will not otherwise affect the Receiving Party's obligations hereunder with respect to Confidential Information so disclosed.

f. **County Data.** All of the County Confidential Information, data, records, and information of County to which Contractor has access, or otherwise provided to Contractor under this Agreement ("County Data"), shall be and remain the property of County and County shall retain exclusive rights and ownership thereto. The data of County shall not be used by Contractor for any purpose other than as required under this Agreement, nor shall such data or any part of

such data be disclosed, sold, assigned, leased, or otherwise disposed of to third-parties by Contractor or commercially exploited or otherwise used by or on behalf of Contractor, its officers, directors, employees, or agents.

g. **Personally Identifiable Information.** "Personally Identifiable Information" shall mean any information that identifies a person, including, but not limited to, name, address, email address, passwords, account numbers, social security numbers, credit card information, personal financial or healthcare information, personal preferences, demographic data, marketing data, credit data, or any other identification data. For the avoidance of doubt, Personally Identifiable Information shall include, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("U.S.C.") §6801 et seq.), Protected Health Information, and "Personally Identifiable Information" as that term is defined in California Civil Code section 1798.29 and EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data.

i. Personally Identifiable Information. In connection with this Agreement and performance of the services, Contractor may be provided or obtain, from County or otherwise, Personally Identifiable Information pertaining to County's current and prospective personnel, directors and officers, agents, subcontractors, investors, patients, and customers and may need to process such Personally Identifiable Information and/or transfer it, all subject to the restrictions set forth in this Agreement and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

ii. Treatment of Personally Identifiable Information. Without limiting any other warranty or obligations specified in this Agreement, and in particular the confidential provisions of Section 21 (County Confidential Information), during the Term of this Agreement and thereafter in perpetuity, Contractor will not gather, store, log, archive, use, or otherwise retain any Personally Identifiable Information in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any Personally Identifiable Information to any third-party, except as expressly required to perform its obligations in this Agreement or as Contractor may be expressly directed in advance in writing by County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Agreement, (b) County's then current privacy policy (available at https://intranet.ladhs.org/intracommon/public/DhsPolPro/polProSearchAction.cfm?unit=dhsintra&prog=dhsintra&ou=dhsintra), and (c) all applicable local, state, and federal laws and regulations (including, but not limited to, current and future laws and regulations relating to spamming, privacy, confidentiality, data security, and consumer protection).

iii. Retention of Personally Identifiable Information. Contractor will not retain any Personally Identifiable Information for any period longer than necessary for Contractor to fulfill its obligations under this Agreement. As soon as Contractor no longer needs to retain such Personally Identifiable Information in order to perform its duties under this

Agreement, Contractor will promptly return or destroy or erase all originals and copies of such Personally Identifiable Information.

h. **Return of Confidential Information.** On County's written request or upon expiration or termination of this Agreement for any reason, Contractor will promptly: (a) return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County's Confidential Information; (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Agreement; and (c) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 13(a), and provide a notarized written statement to County certifying that all documents and materials referred to in Subsections 13(a) and (b) have been delivered to County or destroyed, as requested by County. On termination or expiration of this Agreement, County shall return or destroy all Contractor Confidential Information (excluding items licensed to County hereunder or that are required for use of the Deliverables and/or the Licensed Software), at Contractor's option.